SOLUTIONS TO HOMEWORK 7

1. If α is even, then it is evident that g^α is a quadratic residue modulo p. If α is odd, meanwhile, then by Fermat's Little Theorem one has $(g^\alpha)^{(p-1)/2} \equiv g^{(p-1)/2} \pmod p$. Also, since g is primitive, one has $g^{(p-1)/2} \not\equiv 1 \pmod p$, whence $g^{(p-1)/2} \equiv -1 \pmod p$. Then it follows from Euler's criterion that g^α is a quadratic non-residue modulo p. Thus we conclude that (a) g^α is a quadratic residue modulo p if and only if α is even, and (b) g^α is a quadratic non-residue modulo p if and only if α is odd.
(c) The sum of all the quadratic residues distinct modulo p is

$$1 + g^2 + \cdots + g^{p-3} = \frac{g^{p-1} - 1}{g^2 - 1}.$$

But since $p > 3$ one has $(g^2 - 1, p) = 1$, and by Fermat's Little Theorem one has $g^{p-1} \equiv 1 \pmod p$. Thus the sum of all the quadratic non-residues distinct modulo p is congruent to 0 modulo p.

The product of all the quadratic residues distinct modulo p is

$$1 \cdot g^2 \cdot \cdots \cdot g^{p-3} = g^k,$$

where

$$k = \sum_{r=0}^{(p-3)/2} 2r = \left(\tfrac{1}{2}(p-1)\right)\left(\tfrac{1}{2}(p-3)\right).$$

But $g^{(p-1)/2} \equiv -1 \pmod p$, and so we deduce that

$$1 \cdot g^2 \cdot \cdots \cdot g^{p-3} \equiv (g^{(p-1)/2})^{(p-3)/2} \equiv (-1)^{(p-3)/2} \pmod p.$$

So the product of all the quadratic residues distinct modulo p is congruent to $(-1)^{(p-3)/2}$ modulo p.

2. (a) Observe that $2023 = 17^2 \cdot 7$. Hence, when p is an odd prime number with $p \neq 17$, one has

$$\left(\frac{2023}{p}\right) = \left(\frac{17^2 \cdot 7}{p}\right) = \left(\frac{7}{p}\right).$$

(b) One has

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p^2-1)/8}.$$

When $p \equiv 1 \pmod 8$, we have $(p-1)/2 + (p^2-1)/8 \equiv 0 + 0 \equiv 0 \pmod 2$, and when $p \equiv 3 \pmod 8$, we have $(p-1)/2 + (p^2-1)/8 \equiv 1 + 1 \equiv 0 \pmod 2$. Also, when $p \equiv -1 \pmod 8$, we have $(p-1)/2 + (p^2-1)/8 \equiv 1 + 0 \equiv 1 \pmod 2$, and when $p \equiv -3 \pmod 8$, we have $(p-1)/2 + (p^2-1)/8 \equiv 0 + 1 \equiv 1 \pmod 2$. Thus $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$.

3. (a) If a and b are both quadratic non-residues, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$, and hence

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)^2 = 1,$$

so that ab is a quadratic residue.

(b) It follows from part (a) that at least one of the congruences $x^2 \equiv a \pmod{p}$, $x^2 \equiv b \pmod{p}$ and $x^2 \equiv ab \pmod{p}$ is soluble. Thus, we can always choose a value of x for which some one of $x^2 - a$, $x^2 - b$ and $x^2 - ab$ is divisible by p, whence the congruence $(x^2 - a)(x^2 - b)(x^2 - ab) \equiv 0 \pmod{p}$ always possesses a solution x modulo p.

4. (a) Suppose that M_n is prime but n is composite, say $n = ab$ with $1 < a \leqslant b < n$. Then $2^n - 1 = 2^{ab} - 1 = (2^a - 1)(2^{(b-1)a} + 2^{(b-2)a} + \cdots + 1)$, and since a and b both exceed 1, neither of the latter factors is 1. Thus M_n is composite, giving a contradiction. Then whenever M_n is prime we find that n is prime.

(b) Since $p' = 2p + 1$ is prime, we have

$$\left(\frac{2}{p'}\right) = (-1)^{(p'^2-1)/8} = (-1)^{(2p)(2p+2)/8} = (-1)^{p(p+1)/2},$$

so that when $p \equiv 3 \pmod{4}$, we have $\left(\frac{2}{p'}\right) = 1$. But by Euler's Criterion,

$$\left(\frac{2}{p'}\right) \equiv 2^{(p'-1)/2} = 2^p \pmod{p'},$$

and thus we deduce that $2^p \equiv 1 \pmod{p'}$.

(c) Since the prime $251 \equiv 3 \pmod{4}$, and $2 \cdot 251 + 1 = 503$ is prime, we deduce from the above that $503 | (2^{251} - 1)$, whence $2^{251} - 1$ is not a Mersenne prime.